

Forum:[Hack Forums](#)

Thread: [Cursor Autorun Flaw Lets Repositories Execute Code Without Consent](#)

MadScientist - September 14, 2025, 8:50 am

A newly disclosed flaw in the Cursor extension allows repositories to automatically execute code when a folder is opened, even without a developer's consent.

The issue stems from the extension's "autorun" feature, which launches commands tied to workspace events, such as opening a project.

Researchers at Oasis Security found that malicious actors could craft repositories that exploit this functionality. By embedding hidden instructions, attackers can trigger unauthorized code execution the moment a user opens the repository in Visual Studio Code with Cursor installed.

The discovery highlights how supply chain threats are evolving beyond dependency hijacking. Instead of waiting for a developer to run scripts or install packages, adversaries can now weaponize something as routine as opening a folder.

"The Oasis Security team's findings highlight a serious but often overlooked risk: the silent execution of malicious code through development environments," said Heath Renfrow, CISO at Fenix24.

Source - <https://www.infosecurity-magazine.com/news/cursor-autorun-flaw-repos-execute/>